

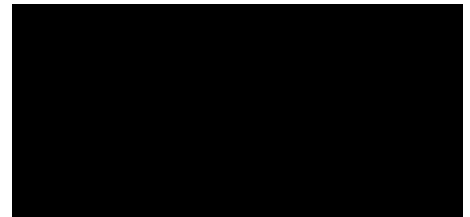
Siemens Healthcare GmbH, SHS AT RO PT QT, Hofmannstr. 26, 91052 Erlangen

To all users of IONTRIS, syngo RT Planning System

Name
Dept.

Telephon
Mobil
E-Mail

Your reference
Our reference
Date



July 18th 2019

Customer Safety Advisory Notice

PT027/18/S

IONTRIS (10013850, 10013851 Siemens AG)
syngo RT Planning System (10652106, Siemens AG)

Potential Patient Hazards Due to Vulnerability in Microsoft Operating Systems

Dear Customer,

with this letter we would like to inform you about a gap in Microsoft operating systems with Remote Desktop Services (Microsoft Security Update CVE-2019-0708, Remote Desktop Services Remote Code Execution Vulnerability, May 14, 2019 at: <https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708>.) and, as a result, the unlikely but possible risk to patient.

When can this vulnerability cause a malfunction and what are the potential risks?

Remote Desktop Services (using TCP default port 3389) - formerly known as Terminal Services - has a remote code execution vulnerability in Remote Desktop Protocol (RDP). The vulnerability lies in the possibility of 'pre-authentication', i.e. login can be done without further user interaction. An attacker who successfully exploited this vulnerability could potentially run arbitrary code on the target system, install programs, view, modify, or delete data, or create new user accounts with full user rights.

This vulnerability affects unsupported but still widely used Windows operating systems such as XP and Windows Server 2003, as well as supported versions of Windows, including Windows 7 and Windows Server 2008/2008 R2.

So far, no incident has been reported by any PT system in which a cyberattack is the cause. Microsoft is also not aware of specific incident regarding the reported vulnerability.

Currently there are no consequences for patient treatment.

Siemens Healthcare GmbH
Management: Bernhard Montag, Chairman;
Jochen Schmitz, Michael Reitermann

Hofmannstr. 26
91052 Erlangen
Germany

Tel.: +49 (9131) 7 0
siemens.com/healthcare

Chairman of the Supervisory Board: Michael Sen
Registered office: Munich, Germany; Commercial Registry: Munich, HRB 213821
WEEE-Reg.-No. DE 64872105

What steps can the user take to prevent the potential risk to the user?

- Disable the Remote Desktop Protocol (RDP).
- Make sure you have appropriate backups and system recovery procedures.
- Comply with the warnings and precautions in accordance with the instructions of the operator's manuals:

<i>IONTRIS (10013850)</i>		Print-Number PT01-...	
Manual	Chapter	German	English/Chinese/Italian
Betreiberhandbuch VA11	8 (Sicherheit - Virenschutz)	SOM.629.02.05.01	n.a.
Betreiberhandbuch VA12	8 (Sicherheit - Virenschutz)	SOM.629.03.06.01	n.a.
syngo PT Treatment VA10A	3 (Sicherheit -Konfiguration und Modifikation des Systems/Schutz vor Viren)	TRM.621.01.01.01	n.a.
Medical Physicist Application VA11A	3 (Sicherheit -Konfiguration und Modifikation des Systems/Schutz vor Viren)	MPA.621.01.01.01	n.a.

<i>IONTRIS (10013851)</i>		Print-Number PT02-...			
Manual	Chapter	German	English	Chinese	Italian
System Owner Manual VB11	8 (Facility Safety - Virus protection)	SOM.629.02.06.01	SOM.629.03.12.02	SOM.629.03.12.21	n.a.
syngo PT Treatment Suite	3 (Safety - Configuration and System Modification / Virus Protection)	TRM.621.02.07.01	TRM.621.02.14.02	TRM.621.02.14.21	n.a.
PT QA & Service VB11	3 (Safety - Configuration and System Modification / Virus Protection)	MPA.621.02.04.01	MPA.621.02.09.02	MPA.621.02.09.21	n.a.

<i>syngo RT Planning System (10652106)</i>		Print-Number T11-...			
Manual	Chapter	German	English	Chinese	Italian
User Manual VC10	A (Safety - Unauthorized Manipulation of the System)	050.621.20.02.01	050.621.20.02.02	050.621.20.02.21	050.621.20.02.11
User Manual VC13	A (Safety - Unauthorized Manipulation of the System)	050.621.40.01.01	050.621.40.01.02	050.621.40.01.21	050.621.40.01.11

What adjustments are made by the manufacturer?

All affected computers were evaluated as to whether deactivation of the RDP service or activation of the Network Level Authentication (NLA) can be performed.

The deactivation of the RDP as well as the activation of the NLA will be implemented as a solution together with the delivery of this customer information (PT010/19/S). The prerequisite for this solution to be implemented is a domain access authorization for Siemens Healthineers. If this is not possible, the implementation is the responsibility of the customer.

This action closes the vulnerability in Microsoft operating systems with Remote Desktop Services.

Future updates will include the Microsoft patch CVE-2019-0708 or there will be an upgrade to an unaffected operating system.

Passing on the information described here:

Please make sure in your organization that all users of the above-mentioned products and other persons to be informed of this safety information. If you have given the products to third parties, please forward a copy of this information or inform the contact person listed below

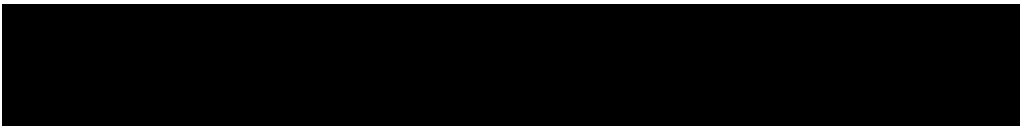
Please retain this information at least until the action is completed.

The German National Competent Authority has received a copy of this safety advisory notice.

Contact:

Dr. Thomas Uhl
Tel.: +49 9131 84-2550
Mobil: +49 173 7040210
Email: thomas.tu.uhl@siemens-healthineers.com

With best regards,



Siemens Healthcare GmbH

Acknowledgment of receipt

Address:

— As the responsible operator of _____ we hereby confirm that we have read and understood the safety information “**Potential Patient Hazards Due to Vulnerability in Microsoft Operating Systems**”.

Place, Date: _____

Name: _____

Signature: _____